Foto: Monşter; thinkstockphotos.com / Kapsch

Robert Jankovics

Über die Digitalisierung aller Branchen

IT-Sicherheit 4.0

Der Wunsch einer allgegenwärtigen Verfügbarkeit von Informationen aus jeglichen Lebensbereichen führt dazu Informationen in Echtzeit durch IT-Unterstützung zu sammeln, zu verarbeiten und an anderer Stelle für die Konsumation wieder bereitzustellen. Aus dieser Tatsache heraus hat sich eine Bewegung ergeben die nicht mehr aufzuhalten ist, und die ihren Weg aller Wahrscheinlichkeit nach weiter fortsetzen wird - die Digitalisierung aller Lebensbereiche, und umgelegt auf unser Wirtschaftsleben, die Digitalisierung aller Branchen. Doch wo viel Licht scheint fällt auch viel Schatten, und so gehen mit allen Annehmlichkeiten dieser Entwicklung auch viele Risiken und Notwendigkeiten für neue Sicherheitslösungen einher.

Industrie 4.0 ist in der Realität angekommen

Im Februar 2015 erschien ein ausführliches Interview mit Herrn Siegfried Russwurm über die Folgen der Digitalisierung für die Arbeitswelt in der Wochenzeitung „Die Zeit". Herr Russwurm bekleidet eine Doppelfunktion im Vorstand der Siemens AG.

Er forciert als Chief Technical Officer die Digitalisierung aller Geschäfte (Züge, Kraftwerke, Stromübertragung, Medizintechnik, Fabrikautomatisierung, Kfz-Elektrik), während er sich gleichzeitig als Personalchef um die Folgen für 350.000 Beschäftigte im Konzern kümmert. Über 4,4 Milliarden Euro wird Siemens 2015 für Forschung und Entwicklung investieren, einen Großteil davon in „digitale Themen". [1]

Herr Russwurms Einblicke lassen erkennen in welchem Wandel sich die Industrie derzeit befindet. Das Internet of Things findet Anwendung in Roboter und Maschinen von Fertigungsstraßen, in RFID Tag versehenen Einzelbauteilen, und in Fertigungsprozess übergreifenden Monitoring- und Steuerungs-Systemen. Diese Einzelteile fügen sich am Ende der Entwicklung zu einem Wandel der Produktion zusammen, der derzeit unter dem Begriff Industrie 4.0 subsummiert wird. Siemens befindet sich in dieser Entwicklung in breiter Gesellschaft vieler Industrietreibenden.

So melden Aufzüge von Thyssenkrupp beispielsweise bereits vorab selbstständig, wann welcher Teil als nächstes gewartet werden muss, oder bieten intelligente Funktionen an wie eine Missbrauchserkennung oder eine selbsttätige Wiederbelebung im Störungsfall.

Der digitale Umbruch betrifft alle Bereiche

Längst ist von dieser Entwicklung jedoch nicht mehr nur die Industrie, die in einer Smart Factory intelligente Produkte mit eigenen digitalen Identitäten produziert, betroffen. Vielmehr ist die Digitalisierung der uns umgebenden Welt in allen Bereichen zu beobachten. Als Beispiele aus unterschiedlichen Branchen seien die folgenden genannt:

- Health & Life Science: Mit etwas Vorlaufzeit aber doch hat die elektronische Gesundheitsakte ELGA ihren Dienst aufgenommen und stellt medizinischem Personal, sowie dem Patienten, Gesundheitsdaten orts- und

zeitunabhängig zur Verfügung. Im Life Style Sektor erobern zeitgleich sogenannte Wearables, mit Sensoren vernetzte Kleidung und Gadgets, den privaten Health Bereich.

- End-Consumer Services: Den Anwendungsfällen scheinen hier keine Grenzen gesetzt zu sein. Derzeit erschließen Smartphone Apps verstärkt neue Geschäftsfelder im Personentransport. Durch die Anwendungen werden klassische Vermittlungszentralen (und deren Vermittlungsprovisionen) ausgespart, wie das neu am Markt auftretende Transportunternehmen Uber oder die Teilnahme traditioneller Taxi Fahrer an der Vermittlungs-App myTaxi demonstrieren. Dem Anwender werden der Standort des nächsten Wagens und die voraussichtlichen Kosten vor der 1-Klick-Bestellung am Smart Phone dargestellt, sowie alsdann die Wartezeit durch die Echtzeitvisualisierung des herannähernden Wagens per GPS Tracking kurzweilig gestaltet.
- M2M – Machine to Machine Kommunikation: M2M Kommunikation wirkt oft im Verborgenen, überall dort wo Maschinen ihren Status an andere Maschinen, entweder zu monitoring Zwecken, oder zum Auslösen von Wartungsintervallen oder Bestellungen, melden. So melden Textilautomaten der Firma Seidensticker beispielsweise den Bestand an Automaten-Hemden direkt an Systeme des zur Nachfüllung der Ware und zur Entleerung des Geldbehälters zuständigen Dienstleister.
- Smarter Cities: Egal ob es sich um den Bereich Transport & Automotive, um Location based Services im individual Konsum, oder um den Bereich intelligenter Energienetze handelt. Alle Teilnehmer am vitalen Stadtleben, sei es als Dienste-Anbieter oder –Konsument, interagieren untereinander in einem impliziten Zusammenleben. Das Ziel von Smarter Cities ist es, die Steuerung dieses Zusammenlebens, durch die weitere Vernetzung von Informationsströmen und der Abstimmung all dieser Bereiche untereinander, Ressourcen optimiert zu gestalten.

Grundlage für diese voranschreitende Digitalisierung ist es, dass eine große Anzahl an Devices (Sensoren, Aktoren, visualisierende Elemente, Kommunikationselemente, ...) miteinander über ein gemeinsames Netzwerk in Verbindung treten. Das Internet der Dinge ist der Grundbaustein für alle darauf aufsetzenden Anwendungen. Eine aktuelle Marktstudie prognostiziert daher für das Jahr 2018 ca. 20 Milliarden an IP-fähigen Devices.

Traditionelle Sicherheitslösungen greifen nicht mehr

Die tiefe Verwurzelung digitaler Systeme lässt erahnen, dass eine ordnungsgemäße Funktion dieser essentiell ist, und ernstzunehmende Folgeschäden drohen wenn Störungen aufgrund eines breitflächigen Virenbefalls auftreten, oder schlimmer, durch gezielte Manipulation erfolgen.

Begleitend zur Digitalisierung entstehen neue Sicherheitsherausforderungen und das Verlangen nach angemessenen Lösungen. Traditionelle Betrachtungsweisen, die oftmals auf dem Paradigma eines vertrauenswürdigen, internen Netzwerkbereichs basieren, und dessen Kommunikationsregeln über eine klassische Firewall abgebildet werden, funktionieren nicht länger. In einer Welt in der Schnittstellen, Sensoren und Displays in hoher Anzahl an öffentlichen Orten verbaut sind, und in der Dienste auf einer Vielzahl an unterschiedlichen und mobilen Endgeräten konsumiert werden wollen, ist das Trennen zwischen intern und extern, und das fixe Verdrahten von Kommunikationswegen schlichtweg nicht mehr möglich. Ähnliches gilt für das Unterscheiden zwischen bösartigen und nicht bösartigen Inhalten in modernen Kommunikationsnetzen.

Lange schon arbeiten Autoren von Viren, Malware und Trojanern mit ausgefeilten Verschleierungstechniken daran die Erkennungsrate von klassischen Antiviren-Schutzprogrammen zu senken. Und das leider mit nicht zu verachtendem Erfolg. Pattern basierende Erkennungsalgorithmen scheitern zunehmend an sich selbstständig verändernden Schadcode (Polymorphismus), Verschlüsselung (encrypted payload) und komplexen Angriffsmustern (z.B. Trennung von Erstinfektion und nachladen von tatsächlichem Schadcode).

Neue Sicherheitskonzepte sind gefordert

Die erfreuliche Nachricht lautet, dass der Markt für Sicherheitslösungen bereits innovative Produkte und Konzepte zur Verfügung stellt. Die Bandbreite dabei ist breit gefächert und bietet einen Mix aus konzeptionellen Ansätzen und Technologie. Die Herausforderung besteht darin für das eigene Betätigungsfeld die richtige Auswahl der zur Verfügung stehenden Ideen zu einer sinnvollen Gesamtlösung zusammen zu führen. Die folgenden Konzepte und Technologien können Bestandteil einer solchen Gesamtlösung sein:

- Netzwerksegmentierung: Die klassische Aufteilung zwischen einem internen und einem öffentlichen Netzbereich greift zu kurz. Eine Segmentierung in funktionsbedingte Netzbereiche schafft eine Kapselung in Vertrauenszonen mit definierten Schnittstellen zu anderen Segmenten hin.

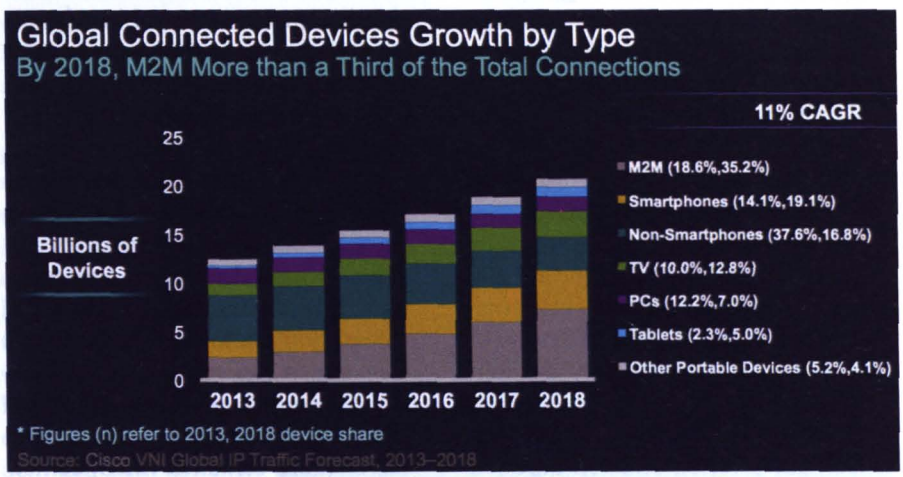
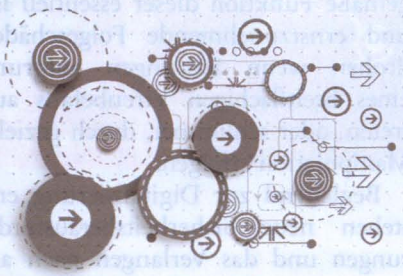


Abbildung 1: Zahlenmässiges Wachstum von IP fähigen Geräten bis 2018

- Next-Generation Firewall: Eine Netzwerksegmentierung macht aus sicherheitstechnischer Sicht nur dann Sinn, wenn die Segmentübergänge durch Firewalls reglementiert werden. NG Firewalls bieten über das reine Abbilden einer Kommunikationsmatrix hinaus, die Möglichkeit auf Benutzer Rollen (Administrator, Mitarbeiter, Partner, Konsument) und/oder auf Anwendungsebene (nicht alles was auf Port 443 erreichbar ist bietet eine Webseite an, es kann sich auch um ein Service für den P2P File Transfer handeln) einzuschränken.
- SCADA-/Modbus-/Feldbus-Firewall: Speziell im Industrie und Automatisierungstechnik Umfeld werden spezielle Kommunikationsprotokolle eingesetzt (z.B. IEC 60870-5-104, Anwendungsbezogene Norm für Fernwirkaufgaben in IP-Netzen). Da diese Protokolle aus Zeiten hoher physischer Abschottungen stammen, unterstützen sie in der Regel keine Security-Mechanismen (Authentifizierung, Verschlüsselung, Schutz gegen Replay-Attacken, ..). Um diese Protokolle dennoch entsprechend sicher zu betreiben, bieten spezielle Firewall Hersteller Module für diese Industrieprotokolle an.
- Malware & APT (Advanced Persistent Threat) Protection: APT Protection Lösungen werden an neuralgischen Stellen im Netzwerk integriert. Schadcode, der sich über das Netzwerk bewegt, wird durch unterschiedliche Erkennungsalgorithmen identifiziert. Darunter fallen neben der klassischen Pattern basierten Erkennung, das Analysieren des dynamischen Verhaltens zur Laufzeit (Sandboxing), sowie das Abgleichen mit einer umfangreichen Cloud basierten Intelligence Datenbank, in der Charakteristika aktueller Angriffswellen weltweit gesammelt werden.
- 2-Faktor- und Cloud Authentifizierung: In vielen Bereichen beschränkt sich die Zugangskontrolle zu Netzwerkdiensten alleine auf gültige Zugangsdaten mit Benutzername und Passwort. Das Problem wird in letzter Zeit vor allem dadurch verschärft, dass viele Benutzer ihre beruflich eingesetzten Passwörter auch auf diversen anderen Portalen und Cloud-Diensten verwenden. Ein Security-Breach dieser Dienste stellt ohne 2-Faktor Authentifizierung auch ein Sicherheitsrisiko für eigene Zugänge dar. Authentifizierungsverfahren für Cloud Dienste die es erlauben gegen ein firmeninternes Verzeichnis zu authentifizieren (OAuth, SAML), und die Übertragung über das Internet dadurch obsolet machen, werden noch nicht flächendeckend eingesetzt.



- Innovative Endpoint Security Lösungen: Neben klassischen Antiviren-Lösungen existieren eine Reihe weiterer Ansätze Endarbeitsplätze sicherer zu gestalten. Einige von diesen Lösungen setzen auf Verhaltens basierte Erkennungsalgorithmen. Sogenannte Ransomware, das ist Schadsoftware die das befallene System mutwillig unbrauchbar machen (z.B. alle Benutzerdateien auf lokalen Festplatten und auf Netzlaufwerken verschlüsseln) und erst nach Aufforderung einer Lösegeldzahlung die Wiederfreigabe versprechen, ist eindeutig an ihrem Verhaltensmuster zu erkennen. Das Verhalten der Schadsoftware kennzeichnet sich durch sequentielle Verschlüsselungsoperationen vieler Dateien aus, und kann durch das markante Verhalten identifiziert und blockiert werden. Andere Lösungen bauen darauf auf Systeme wie zum Beispiel einen Steuerungs-PC in einem definierten Zustand einzufrieren und allen darüber hinaus laufenden Prozessen die Netzwerkkommunikation oder Interaktion mit lokalen Dateien und Ressourcen zu untersagen. Technisch gesprochen handelt es sich dabei um einen Kernel-Level Filter der das erlaubte Verhalten von Systemen sehr granular spezifizieren lässt.

Die Darstellung geeigneter Sicherheitsmaßnahmen lässt sich weiter fortführen, und jede Technologie muss vor allem in organisatorische Prozesse eingebettet werden um einen sicheren Betrieb zu gewährleisten. In einer wirtschaftlichen Betrachtung muss jedenfalls die Frage gestellt werden, an welcher Stelle ein Investment in Sicherheit am sinnvollsten getätigt ist. Eine geeignete Herangehensweise an diese Bewertung ist die Einführung eines Information Risk Managements (IRM) das Geschäftsrisiken auf technische Risiken herunterbricht und vice versa. Mit der Einführung eines IRM lassen sich Risiken der Informationstechnologie wirtschaftlich fassen und durch die Überführung in ein allenfalls bereits vorhandenes Enterprise Risk Management (ERM) als Geschäftsrisiko ebengleich wie andere Marktrisiken behandeln.

Der geeignete Technologiepartner

Die beschriebenen Aspekte der Digitalisierung beobachten wir bei dem überwiegenden Großteil unserer Kunden in allen Branchensegmenten. Kapsch BusinessCom versteht sich im Zuge dessen als Technologie Partner.

Wir empfehlen unseren Kunden nicht welche Geschäftsfelder sie erschließen sollen oder auf welche Art und Weise das am besten gelingt. In der Transformation einer existierenden Geschäftsvision zu einem konkret ausgestalteten und Technologie gestützten Geschäftsprozess jedoch, sehen wir unsere Kernkompetenz. Das bestehende Portfolio deckt dabei von der vollständige Kette, angefangen bei der eigentlichen Prozesstransformation und -ausgestaltung, über die Implementierung in entsprechend sichere Technologien, bis hin zum operativen und sicheren Betrieb, alle Elemente ab.

Autor:

Dipl.-Ing. Robert Jankovics hat Wirtschaftsingenieurwesen für Informatik an der TU Wien studiert und sich bereits im Laufe seines Studiums auf Informationssicherheit spezialisiert.
Als Teamlead für den Bereich Security Audit & Assessment bei Kapsch BusinessCom beschäftigt er sich intensiv mit dem Themengebiet aktueller Sicherheitsbedrohungen.

Quellenangaben:

[1] DIE ZEIT N° 04/2015, Artikel „DIGITALISIERUNG: „Da bin ich Optimist", Autor DIETMAR H. LAMPARTER

Abbildungen

Grafik 1:
Monster; thinkstockphotos.com / Kapsch

Grafik 2:
http://blogs.cisco.com/news/cisco-visual-networking-index-vni-global-ip-traffic-and-service-adoption-forecast-update-2013-2018
Grafik 3:
KrulUA; thinkstockphotos.com

Dipl.-Ing.

Robert Jankovics

Teamlead
Security Audit
Kapsch BusinessCom

Bernhard Bauer

Einblick in die Welt der Bauingenieure an der TU Graz – Die BIT-BAU'14

Das Institut für Baubetrieb und Bauwirtschaft veranstaltete am 6. November 2014 bereits zum achten Mal den Berufs- und Informationstag Bau, die BIT-BAU'14 an der TU Graz.

Diese in Österreich einzigartige Studien- und Berufsmesse für die Baubranche sprengte auch heuer wieder alle Besucherrekorde. Mehr als 600 Studierenden, Absolventinnen und Absolventen, sowie Schülerinnen und Schülern aus ganz Österreich wurde das breite Anwendungsspektrum des Bauingenieurwesens präsentiert. Auch der Andrang seitens der Aussteller war enorm. So mussten aufgrund von begrenzten Platzverhältnissen erstmals Absagen erteilt und die Zahl der Firmen auf 22 beschränkt werden. Diese Vertreter der Wirtschaft (aus allen DACH Ländern) stellten ihr Betätigungsfeld und Arbeitsgebiet vor und spannten den Bogen von Systemlieferanten, Planungsbüros hin zu ausführenden Unternehmen sowie öffentlichen Auftraggebern. Dabei standen den Besuchern operative Mitarbeiterinnen und Mitarbeiter, aber auch Vertretungen der Geschäftsleitungen und Personalabteilungen der Unternehmungen Rede und Antwort und hatten auch wieder einige Jobs und Praktika im Gepäck.

Abseits des regen Treibens der Messe erhielten Schülerinnen und Schüler bei den begleitenden Vorträgen alle Informationen zum Studium und hatten die Möglichkeit in einem vom Institut ausgelobten Wettbewerb die „Brückenbau-Reife" zu erlangen.

Die 37 eingereichten Konstruktionen aus (vorgegebenen) 500 Trinkhalmen mussten dabei eine Weite von 2 Metern überspannen. Die präsentierten Brückenbauwerke waren in ihrer Kreativität und Vielfalt kaum zu schlagen, nur in ihrer Stabilität waren Unterschiede zu erkennen. So konnte sich mit einer maximalen Traglast von 50 und 30 Kilogramm (Messergebnis nach genormtem Belastungstest) die HTL Ortweinschule gleich die beiden Bestplatzierungen sichern und verwies die Schulen aus Villach, Wels, Linz, Mödling und Zeltweg auf die Ränge.

Die von den Schülern gewonnenen Preise erstreckten sich dabei von einer Klassenreise inkl. Architekurführung durch Graz (sponsored by Landesinnung Bau) über einen Bewerbungsworkshop (sponsored by Personos) bis hin zu einer Exkursionen zu den Brückenbaustellen der Tunnelkette Klaus (sponsored by Asfinag), sodass auch die teilweise weniger erfolgreichen Klassenkollegen der Gewinnerteams einen Grund zum Feiern hatten.

„Wir sehen in der Berufsmesse die Chance, unsere Studierenden bereits im Rahmen ihrer Ausbildung an die Praxis heranzuführen bzw. den Schülerinnen und Schülern das mögliche zukünftige Betätigungsfeld näher zu bringen", so die Veranstalter Prof. Dr.-Ing. Detlef Heck, DDipl.-Ing. Bernhard Bauer und Dipl.-Ing. Jörg Koppelhuber.

Fotos und weitere Informationen zur Messe, sind unter www.bit-bau.at und https://www.facebook.com/media/set/?set=a.566777686801335.1073741831.145488238930284&type=1 zu finden.